UNIT- III

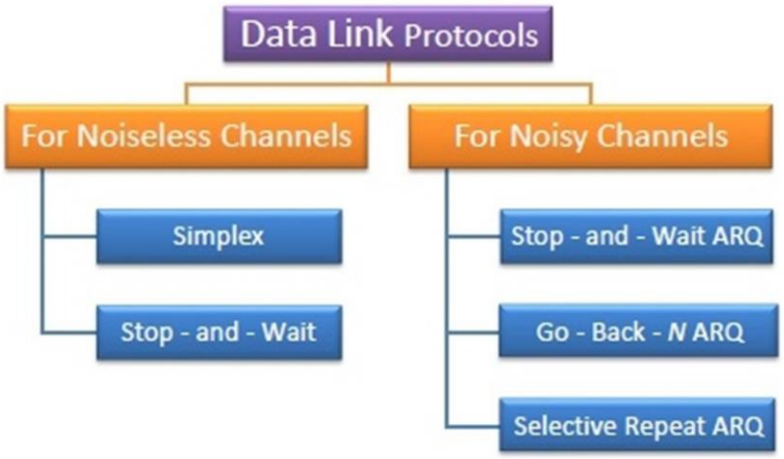
1. Elementary data link layer protocols

Protocols in the data link layer are designed so that this layer can perform its basic functions: framing, error control and flow control. Framing is the process of dividing bit - streams from physical layer into data frames whose size ranges from a few hundred to a few thousand bytes.

Error control mechanisms deals with transmission errors and retransmission of corrupted and lost frames. Flow control regulates speed of delivery and so that a fast sender does not drown a slow receiver.

Types of Data Link Protocols

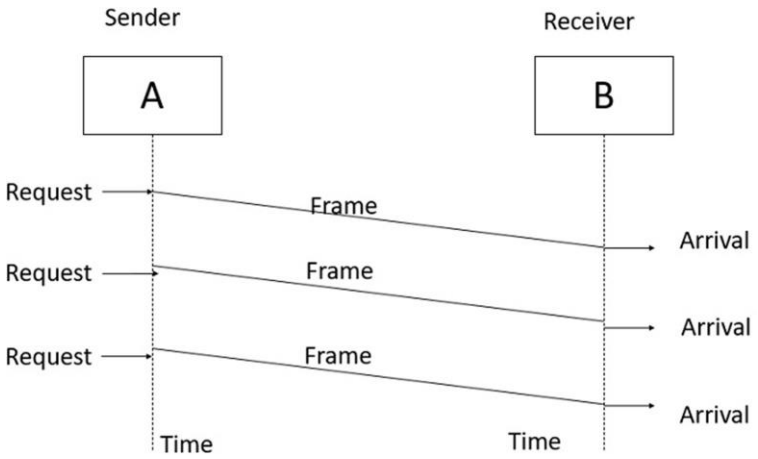
Data link protocols can be broadly divided into two categories, depending on whether the transmission channel is noiseless or noisy.



Simplex Protocol

- Data transmitting is carried out in one direction only. The transmission (Tx) and receiving (Rx) are always ready and the processing time can be ignored.
- In this protocol, infinite buffer space is available, and no errors are occurring that is no damage frames and no lost frames.
- The Simplex protocol is hypothetical protocol designed for unidirectional data transmission over an ideal channel, i.e. a channel through which transmission can never go wrong.

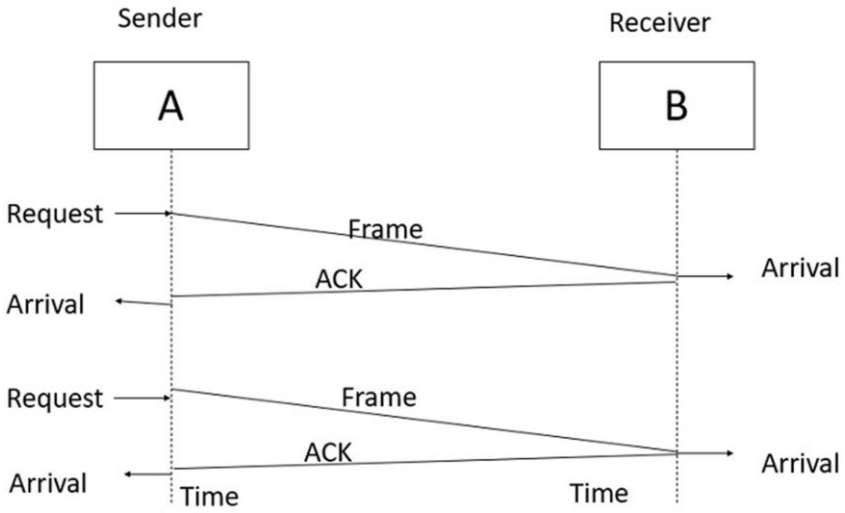
- It has distinct procedures for sender and receiver. The sender simply sends all its data available onto the channel as soon as they are available its buffer.
- The receiver is assumed to process all incoming data instantly. It is hypothetical since it does not handle flow control or error control.



Simplex Stop and Wait protocol

- Stop – and – Wait protocol is for noiseless channel too. It provides unidirectional data transmission without any error control facilities.
- However, it provides for flow control so that a fast sender does not drown a slow receiver. The receiver has a finite buffer size with finite processing speed.
- The sender can send a frame only when it has received indication from the receiver that it is available for further data processing.
- In this protocol we assume that data is transmitted in one direction only. No error occurs; the receiver can only process the received information at finite rate.
- These assumptions imply that the transmitter cannot send frames a rate faster than the receiver can process them.
- The main problem here is how to prevent the sender from flooding the receiver. The general solution for this problem is to have the receiver send some sort of feedback to sender, the process is as follows –
- **Step1** – The receiver send the acknowledgement frame back to the sender telling the sender that the last received frame has been processed and passed to the host.
- **Step 2** – Permission to send the next frame is granted.
- **Step 3** – The sender after sending the sent frame has to wait for an acknowledge frame from the receiver before sending another frame.

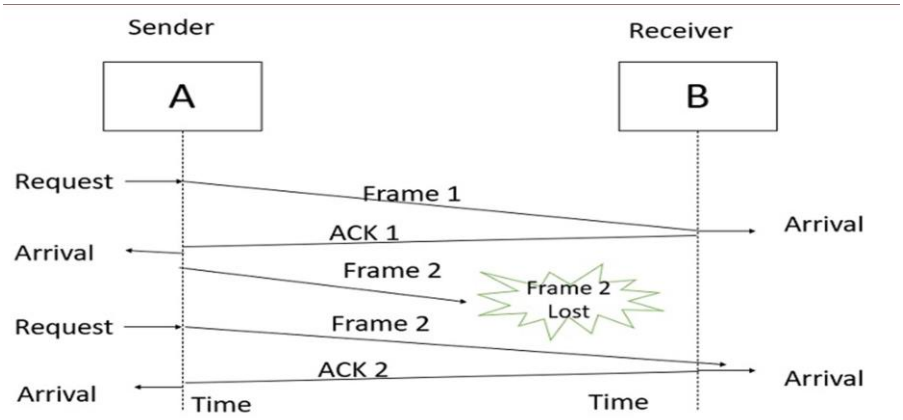
- This protocol is called Simplex Stop and wait protocol, the sender sends one frame and waits for feedback from the receiver. When the ACK arrives, the sender sends the next frame.
- The Simplex Stop and Wait Protocol is diagrammatically represented as follows –



Simplex Protocol for Noisy Channel

Stop – and – wait Automatic Repeat Request (Stop – and – Wait ARQ)

- **Stop – and – Wait ARQ** is a variation of the above protocol with added error control mechanisms, appropriate for noisy channels. The sender keeps a copy of the sent frame.
- It then waits for a finite time to receive a positive acknowledgement from receiver. If the timer expires or a negative acknowledgement is received, the frame is retransmitted.
- If a positive acknowledgement is received then the next frame is sent.
- Data transfer is only in one direction, consider separate sender and receiver, finite processing capacity and speed at the receiver, since it is a noisy channel, errors in data frames or acknowledgement frames are expected.
- Every frame has a unique sequence number.
- After a frame has been transmitted, the timer is started for a finite time.
- Before the timer expires, if the acknowledgement is not received , the frame gets retransmitted, when the acknowledgement gets corrupted or sent data frames gets damaged, how long the sender should wait to transmit the next frame is infinite.
- The Simplex Protocol for Noisy Channel is diagrammatically represented as follows –



2. Sliding Window Protocol

- The sliding window is a technique for sending multiple frames at a time.
- It controls the data packets between the two devices where reliable and gradual delivery of data frames is needed.
- It is also used in TCP (Transmission Control Protocol).
- In this technique, each frame has sent from the sequence number.
- The sequence numbers are used to find the missing data in the receiver end.
- The purpose of the sliding window technique is to avoid duplicate data, so it uses the sequence number.

Types of Sliding Window Protocol

Sliding window protocol has two types:

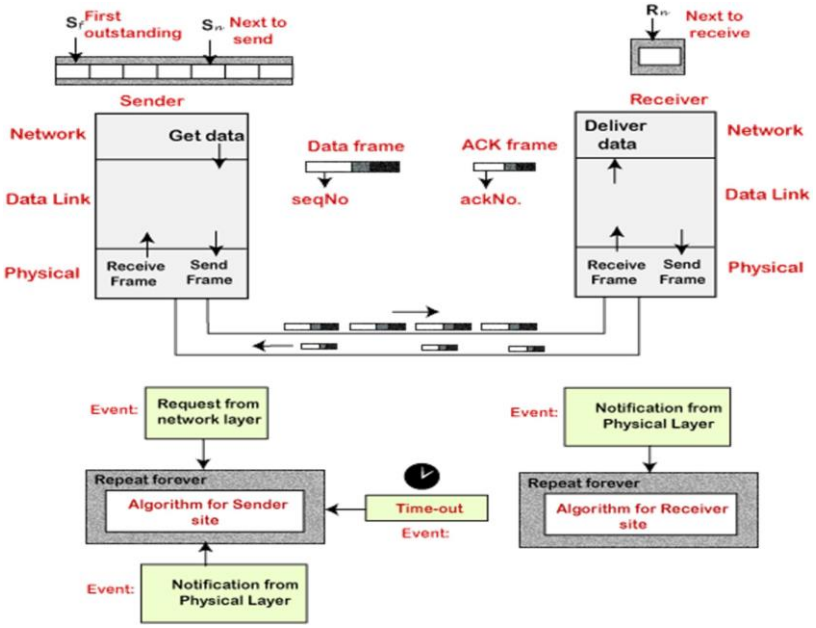
1. **Go-Back-N ARQ**
2. **Selective Repeat ARQ**

Go-Back-N ARQ

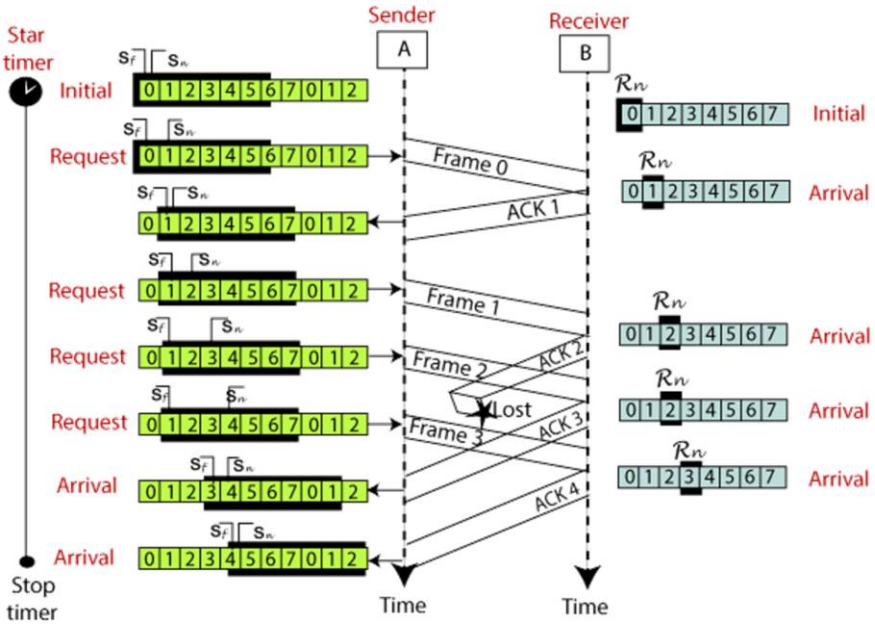
Go – Back – N ARQ provides for sending multiple frames before receiving the acknowledgement for the first frame. It uses the concept of sliding window, and so is also called sliding window protocol. The frames are sequentially numbered and a finite number of frames are sent. If the acknowledgement of a frame is not received within the time period, all frames starting from that frame are retransmitted.

- Go-Back-N ARQ protocol is also known as Go-Back-N Automatic Repeat Request.
- It is a data link layer protocol that uses a sliding window method.
- In this, if any frame is corrupted or lost, all subsequent frames have to be sent again.
- The size of the sender window is N in this protocol.
- For example, Go-Back-8, the size of the sender window, will be 8.
- The receiver window size is always 1.
- If the receiver receives a corrupted frame, it cancels it.
- The receiver does not accept a corrupted frame.
- When the timer expires, the sender sends the correct frame again.

- The design of the Go-Back-N ARQ protocol is shown below.

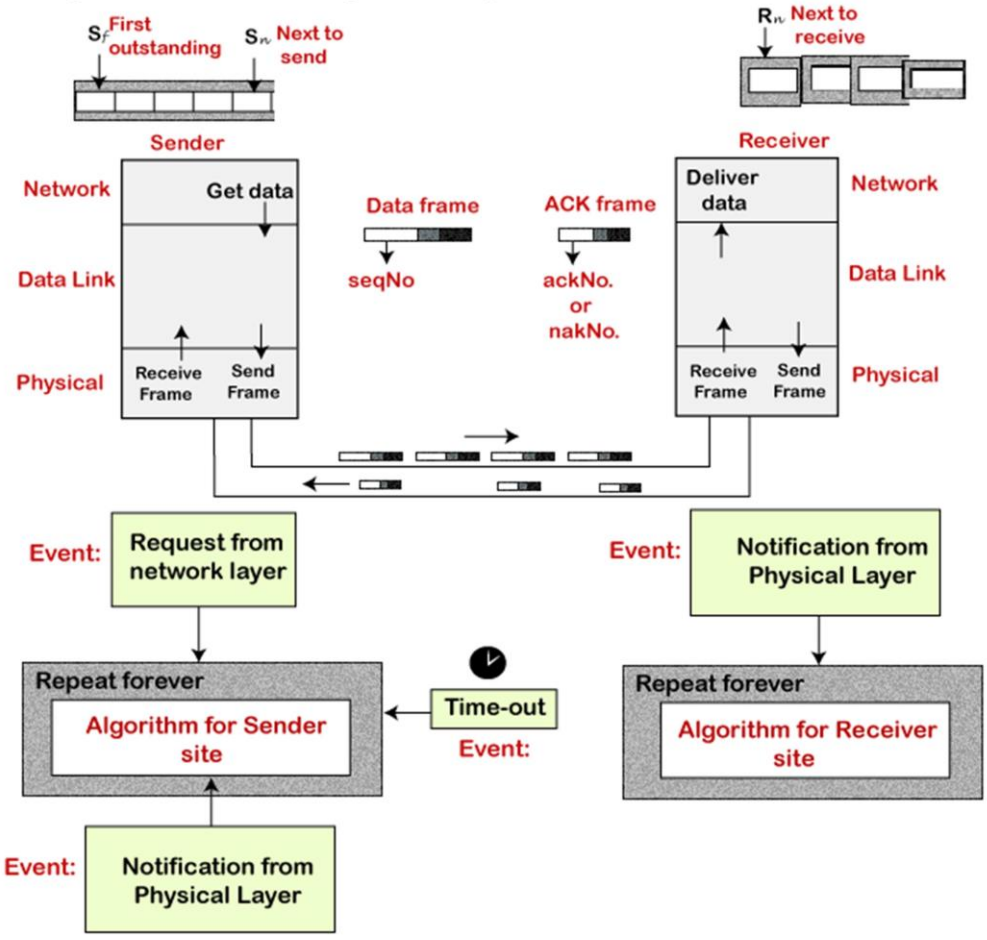


The example of Go-Back-N ARQ is shown below in the figure.

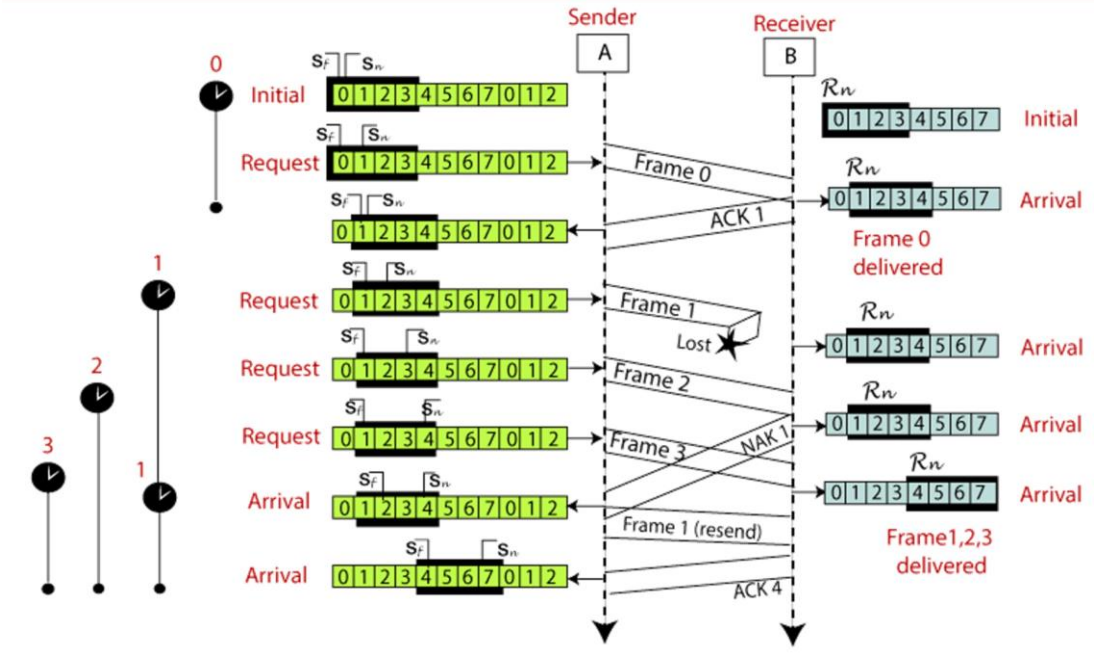


Selective Repeat ARQ

- This protocol also provides for sending multiple frames before receiving the acknowledgement for the first frame. However, here only the erroneous or lost frames are retransmitted, while the good frames are received and buffered.
- Selective Repeat ARQ is also known as the Selective Repeat Automatic Repeat Request.
- It is a data link layer protocol that uses a sliding window method.
- The Go-back-N ARQ protocol works well if it has fewer errors.
- But if there is a lot of error in the frame, lots of bandwidth loss in sending the frames again. So, we use the Selective Repeat ARQ protocol.
- In this protocol, the size of the sender window is always equal to the size of the receiver window.
- The size of the sliding window is always greater than 1.
- If the receiver receives a corrupt frame, it does not directly discard it. It sends a negative acknowledgment to the sender.
- The sender sends that frame again as soon as on the receiving negative acknowledgment.
- There is no waiting for any time-out to send that frame.
- The design of the Selective Repeat ARQ protocol is shown below.



The example of the Selective Repeat ARQ protocol is shown below in the figure.



Difference between the Go-Back-N ARQ and Selective Repeat ARQ

Go-Back-N ARQ	Selective Repeat ARQ
If a frame is corrupted or lost in it,all subsequent frames have to be sent again.	In this, only the frame is sent again, which is corrupted or lost.
If it has a high error rate,it wastes a lot of bandwidth.	There is a loss of low bandwidth.
It is less complex.	It is more complex because it has to do sorting and searching as well. And it also requires more storage.
It does not require sorting.	In this, sorting is done to get the frames in the correct order.
It does not require searching.	The search operation is performed in it.
It is used more.	It is used less because it is more complex.

3. Data Link Layer in the internet

The internet consists of individual systems (host and routers) that are connected to each other. The internet connects the host which resides in the LAN situated in a building. The internet looks like a WAN with point-to-point leased line connection.

The Point-to-point is primarily used in two situations

1. Thousands of organizations having one or more LANs. The hosts in the LANs are connected by many distinct routers. These routers, source and destination hosts are connected using Point-to-Point links.
2. The Individual users are connected to internet with dial-up modems using Point-to-Point link. The home PCs are connected to Internet providers.

PPP Protocol

- The PPP stands for Point-to-Point protocol. It is the most commonly used protocol for point-to-point access. Suppose the user wants to access the internet from the home, the PPP protocol will be used.
- The PPP protocol can be used on synchronous link like ISDN as well as asynchronous link like dial-up. It is mainly used for the communication between the two devices.
- It can be used over many types of physical networks such as serial cable, phone line, trunk line, cellular telephone, fiber optic links such as SONET.

Services provided by PPP

- It defines the format of frames through which the transmission occurs.
- It defines the link establishment process. If user establishes a link with a server, then "how this link establishes" is done by the PPP protocol.
- It defines data exchange process, i.e., how data will be exchanged, the rate of the exchange.
- The main feature of the PPP protocol is the encapsulation. It defines how network layer data and information in the payload are encapsulated in the data link frame.
- It defines the authentication process between the two devices. The authentication between the two devices, handshaking and how the password will be exchanged between two devices are decided by the PPP protocol.

Services Not provided by the PPP protocol

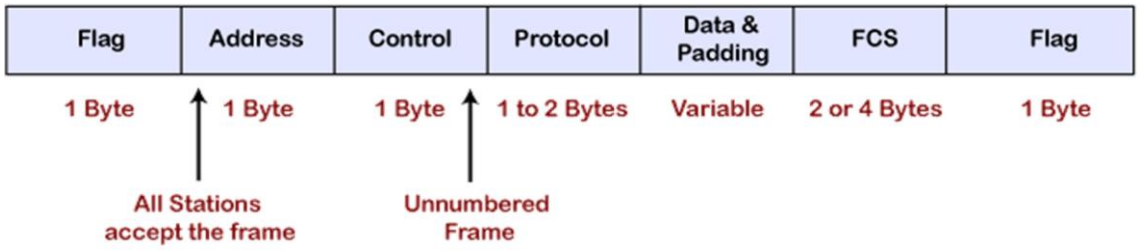
- It does not support flow control mechanism.
- It has a very simple error control mechanism.
- As PPP provides point-to-point communication, so it lacks addressing mechanism to handle frames in multipoint configuration.

PPP has two main uses which are given below:

- It is widely used in broadband communications having heavy loads and high speed. For example, an internet operates on heavy load and high speed.
- It is used to transmit the multiprotocol data between the two connected (point-to-point) computers. It is mainly used in point-to-point devices, for example, routers are point-to-point devices where PPP protocol is widely used as it is a WAN protocol not a simple LAN ethernet protocol.

Frame format of PPP protocol

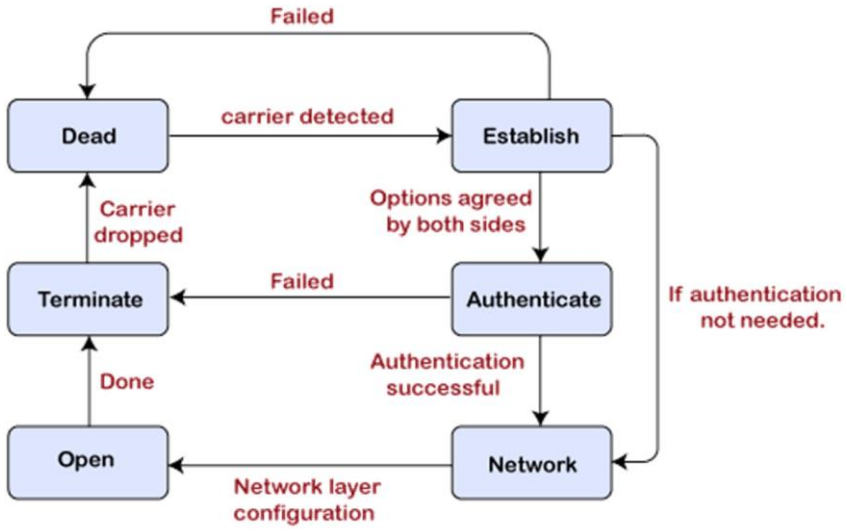
The frame format of PPP protocol contains the following fields:



- **Flag:** The flag field is used to indicate the start and end of the frame. The flag field is a 1-byte field that appears at the beginning and the ending of the frame. The pattern of the flag is similar to the bit pattern in HDLC, i.e., 01111110.
- **Address:** It is a 1-byte field that contains the constant value which is 11111111. These 8 ones represent a broadcast message.
- **Control:** It is a 1-byte field which is set through the constant value, i.e., 11000000. It is not a required field as PPP does not support the flow control and a very limited error control mechanism. The control field is a mandatory field where protocol supports flow and error control mechanism.
- **Protocol:** It is a 1 or 2 bytes field that defines what is to be carried in the data field. The data can be a user data or other information.
- **Payload:** The payload field carries either user data or other information. The maximum length of the payload field is 1500 bytes.
- **Checksum:** It is a 16-bit field which is generally used for error detection.

Transition phases of PPP protocol

- **The following are the transition phases of a PPP protocol:**



Transition phases

  - **Dead:** Dead is a transition phase which means that the link is not used or there is no active carrier at the physical layer.
  - **Establish:** If one of the nodes starts working then the phase goes to the establish phase. In short, we can say that when the node starts communication or carrier is detected then it moves from the dead to the establish phase.
  - **Authenticate:** It is an optional phase which means that the communication can also moves to the authenticate phase. The phase moves from the establish to the authenticate phase only when both the communicating nodes agree to make the communication authenticated.
  - **Network:** Once the authentication is successful, the network is established or phase is network. In this phase, the negotiation of network layer protocols take place.
  - **Open:** After the establishment of the network phase, it moves to the open phase. Here open phase means that the exchange of data takes place. Or we can say that it reaches to the open phase after the configuration of the network layer.
  - **Terminate:** When all the work is done then the connection gets terminated, and it moves to the terminate phase. On reaching the terminate phase, the link moves to the dead phase which indicates that the carrier is dropped which was earlier created.

There are two more possibilities that can exist in the transition phase:

  - The link moves from the authenticate to the terminate phase when the authentication is failed.
  - The link can also move from the establish to the dead state when the carrier is failed.

PPP Stack

In PPP stack, there are three set of protocols:

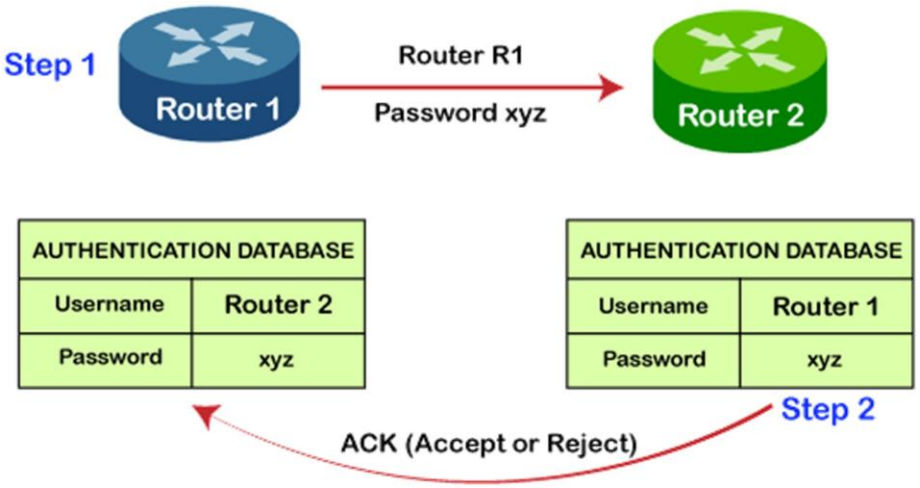
1. Link Control Protocol (LCP)

The role of LCP is to establish, maintain, configure, and terminate the links. It also provides negotiation mechanism.

2. Authentication protocols

There are two types of authentication protocols, i.e., **PAP (Password Authenticate protocols), and CHAP (Challenged Handshake Authentication Protocols).**

1. PAP (Password Authentication Protocols)



- PAP is less secure as compared to CHAP as in case of PAP protocol, password is sent in the form of a clear text. It is a two-step process. Suppose there are two routers, i.e., router 1 and router 2.
- In the first step, the router 1 wants to authenticate so it sends the username and password for the authentication. In the second step, if the username and password are matched then the router 2 will authenticate the router 1 otherwise the authentication failed.

2. CHAP (Challenged Handshake Authentication Protocol)

It provides more security than PAP. In this method, password is kept secret. It is a three-way authentication protocol.

Step 1: System sends a challenge packet to the user. It contains a value, usually a few bytes.

Step 2: Using a predefined functions, a user combines this challenge value with the user password and sends the resultant packet back to the system.

Step 3: System then applies the same function to the password of the user & challenge value, and creates a result. If the result is same as the results sent in the response packet, access is granted, otherwise it is denied.

3. Network Control Protocol (NCP)

After the establishment of the link and authentication, the next step is to connect to the network layer. So, PPP uses another protocol known as network control protocol (NCP). The NCP is a set of protocols that facilitates the encapsulation of data which is coming from the network layer to the PPP frames.

4. Channel Allocation Problem in Computer Networks

In a broadcast network, the single broadcast channel is to be allocated to one transmitting user at a time. When multiple users use a shared network and want to access the same network. Then channel allocation problem in computer networks occurs. So, to allocate the same channel between multiple users, techniques are used, which are called channel allocation techniques in computer networks.

Channel Allocation Techniques

For the efficient use of frequencies, time-slots and bandwidth channel allocation techniques are used. There are three types of channel allocation techniques that you can use to resolve channel allocation problem in computer networks as follows:

- Static channel allocation
- Dynamic channel allocation
- Hybrid channel allocation.

1. Static Channel Allocation

The traditional way of allocating a single channel between multiple users is called static channel allocation. Static channel allocation is also called fixed channel allocation. Such as a telephone channel among many users is a real-life example of static channel allocation.

The frequency division multiplexing (FDM) and time-division multiplexing (TDM) are two examples of static channel allocation. In these methods, either a fixed frequency or fixed time slot is allotted to each user.

2. Dynamic Channel Allocation

The technique in which channels are not permanently allocated to the users is called dynamic channel allocation. In this technique, no fixed frequency or fixed time slot is allotted to the user. The allocation depends upon the traffic. If the traffic increases, more channels are allocated, otherwise fewer channels are allocated to the users.

This technique optimizes bandwidth usage and provides fast data transmission. Dynamic channel allocation is further categorized into two parts as follows:

- Centralized dynamic channel allocation
- Distributed dynamic channel allocation

The following are the assumptions in dynamic channel allocation:

Station Model: Comprises N independent stations with a program for transmission.

Single Channel: A single channel is available for all communication.

Collision: If frames are transmitted at the same time by two or more stations, then the collision occurs.

Continuous or slotted time: There is no master clock that divides time into discrete time intervals.

Carrier or no carrier sense: Stations sense the channel before transmission.

3. **Hybrid Channel Allocation**

The mixture of fixed channel allocation and dynamic channel allocation is called hybrid channel allocation. The total channels are divided into two sets, fixed and dynamic sets.

First, a fixed set of channels is used when the user makes a call. If all fixed sets are busy, then dynamic sets are used. When there is heavy traffic in a network, then hybrid channel allocation is used.

Difference between Static and Dynamic Channel Allocation

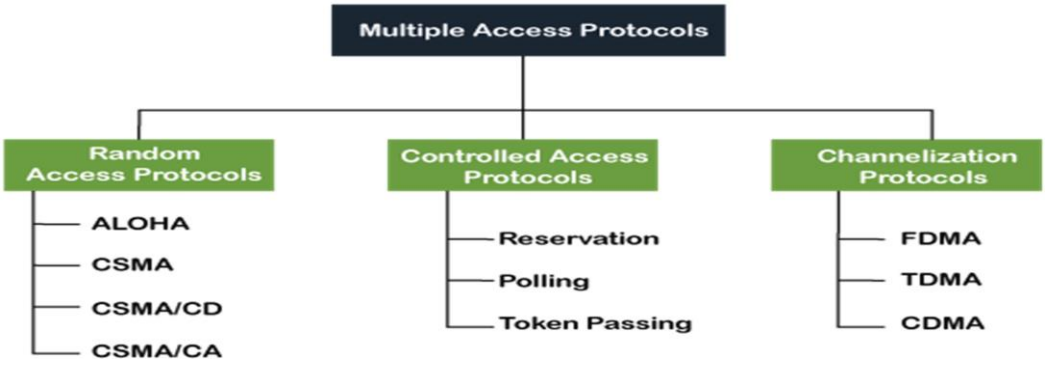
There are some differences between static and dynamic channel allocation. The following table shows the comparison of fixed channel allocation and dynamic channel allocation.

Fixed Channel allocation	**Dynamic Channel allocation**
In this technique, a fixed number of channels are allocated to the cells.	In this technique, channels are not permanently allocated to the cells.
Mobile station centre has fewer responsibilities.	The mobile station centre has more responsibilities.
The allocation is not dependent on traffic.	The allocation depends on the traffic.
Fixed channel allocation is cheaper than dynamic channel allocation.	Dynamic channel allocation is costly as compared to fixed channel allocation.
In this no need of complex algorithms.	Complex algorithms are used in this.

5. **MEDIUM ACCESS PROTOCOLS**

- When a sender and receiver have a dedicated link to transmit data packets, the data link control is enough to handle the channel. Suppose there is no dedicated path to communicate or transfer the data between two devices.

- In that case, multiple stations access the channel and simultaneously transmits the data over the channel. It may create collision and cross talk. Hence, the multiple access protocol is required to reduce the collision and avoid crosstalk between the channels.
- Following are the types of multiple access protocol that is subdivided into the different process as:



A. Random Access Protocol

- In this protocol, all the station has the equal priority to send the data over a channel. In random access protocol, one or more stations cannot depend on another station nor any station control another station.
- Depending on the channel's state (idle or busy), each station transmits the data frame. However, if more than one station sends the data over a channel, there may be a collision or data conflict. Due to the collision, the data frame packets may be lost or changed. And hence, it does not receive by the receiver end.
- Following are the different methods of random-access protocols for broadcasting frames on the channel.
    - **Aloha**
    - **CSMA**
    - **CSMA/CD**
    - **CSMA/CA**

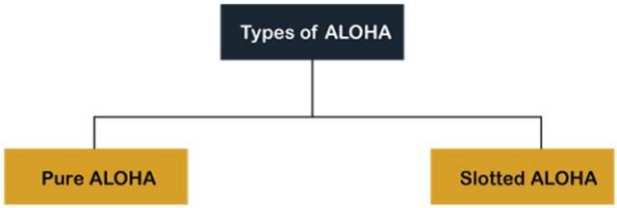
ALOHA Random Access Protocol

It is designed for wireless LAN (Local Area Network) but can also be used in a shared medium to transmit data. Using this method, any station can transmit data across a network simultaneously when a data frameset is available for transmission.

Aloha Rules

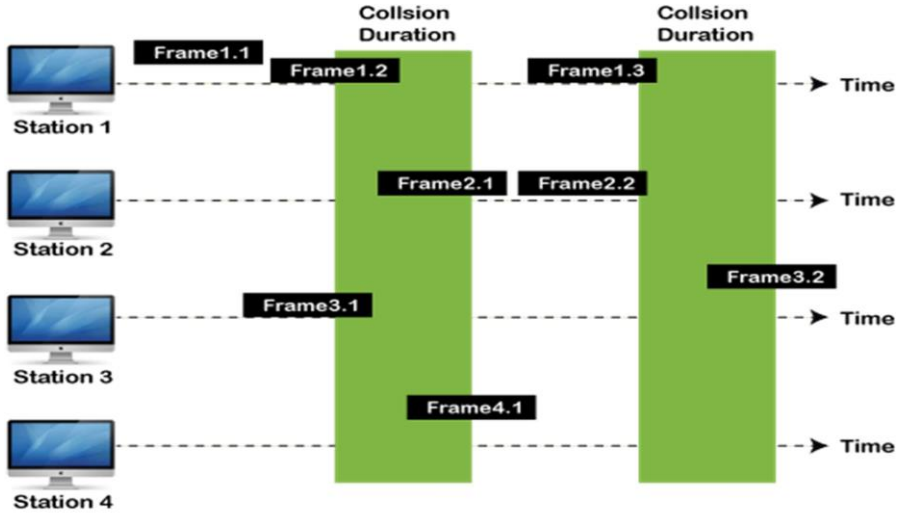
1. Any station can transmit data to a channel at any time.

2. It does not require any carrier sensing.
3. Collision and data frames may be lost during the transmission of data through multiple stations.
4. Acknowledgment of the frames exists in Aloha. Hence, there is no collision detection.
5. It requires retransmission of data after some random amount of time.



Pure Aloha

- Whenever data is available for sending over a channel at stations, we use Pure Aloha. In pure Aloha, when each station transmits data to a channel without checking whether the channel is idle or not, the chances of collision may occur, and the data frame can be lost. When any station transmits the data frame to a channel, the pure Aloha waits for the receiver's acknowledgment. If it does not acknowledge the receiver end within the specified time, the station waits for a random amount of time, called the backoff time (Tb). And the station may assume the frame has been lost or destroyed.
- Therefore, it retransmits the frame until all the data are successfully transmitted to the receiver.
    1. The total vulnerable time of pure Aloha is 2 * Tfr.
    2. Maximum throughput occurs when G = 1/ 2 that is 18.4%.
    3. Successful transmission of data frame is S = G * e ^ - 2 G.



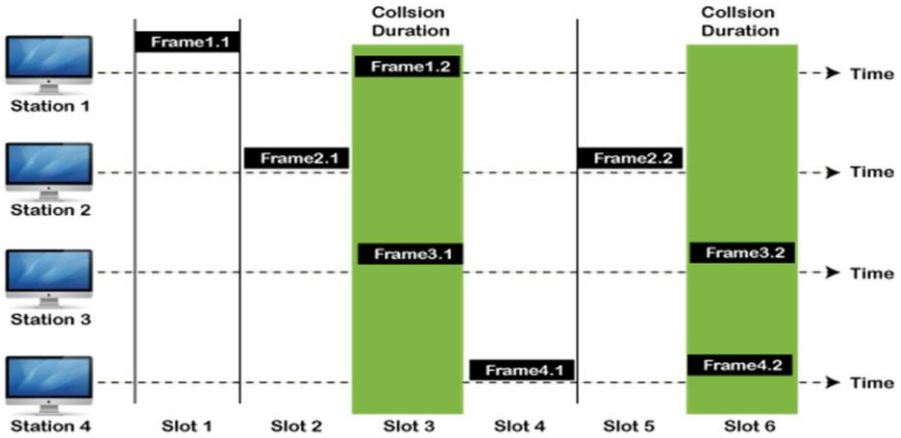
Frames in Pure ALOHA

As we can see in the figure above, there are four stations for accessing a shared channel and transmitting data frames. Some frames collide because most stations send their frames at the same time. Only two frames, frame 1.1 and frame 2.2, are successfully transmitted to the receiver end. At the same time, other frames are lost or destroyed. Whenever two frames fall on a shared channel simultaneously, collisions can occur, and both will suffer damage. If the new frame's first bit enters the channel before finishing the last bit of the second frame. Both frames are completely finished, and both stations must retransmit the data frame.

Slotted Aloha

The slotted Aloha is designed to overcome the pure Aloha's efficiency because pure Aloha has a very high possibility of frame hitting. In slotted Aloha, the shared channel is divided into a fixed time interval called **slots**. So that, if a station wants to send a frame to a shared channel, the frame can only be sent at the beginning of the slot, and only one frame is allowed to be sent to each slot. And if the stations are unable to send data to the beginning of the slot, the station will have to wait until the beginning of the slot for the next time. However, the possibility of a collision remains when trying to send a frame at the beginning of two or more station time slot.

1. Maximum throughput occurs in the slotted Aloha when G = 1 that is 37%.
2. The probability of successfully transmitting the data frame in the slotted Aloha is S = G * e ^ - 2 G.
3. The total vulnerable time required in slotted Aloha is Tfr.



Frames in Slotted ALOHA

CSMA (Carrier Sense Multiple Access)

It is a **carrier sense multiple access** based on media access protocol to sense the traffic on a channel (idle or busy) before transmitting the data. It means that if the channel is idle, the

station can send data to the channel. Otherwise, it must wait until the channel becomes idle. Hence, it reduces the chances of a collision on a transmission medium.

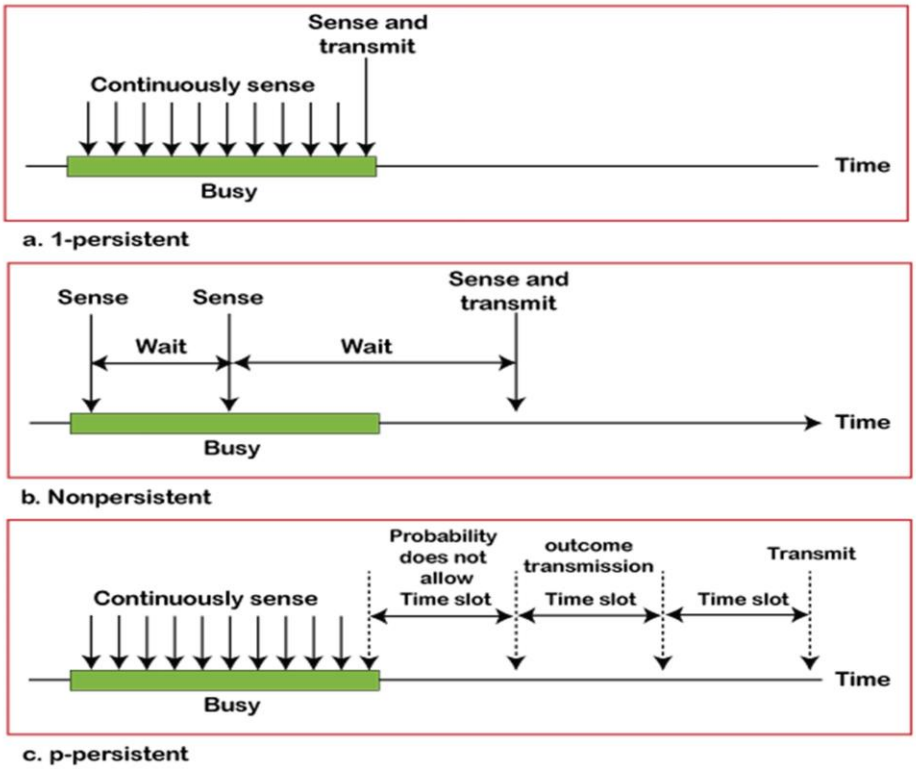
CSMA Access Modes

1-Persistent: In the 1-Persistent mode of CSMA that defines each node, first sense the shared channel and if the channel is idle, it immediately sends the data. Else it must wait and keep track of the status of the channel to be idle and broadcast the frame unconditionally as soon as the channel is idle.

Non-Persistent: It is the access mode of CSMA that defines before transmitting the data, each node must sense the channel, and if the channel is inactive, it immediately sends the data. Otherwise, the station must wait for a random time (not continuously), and when the channel is found to be idle, it transmits the frames.

P-Persistent: It is the combination of 1-Persistent and Non-persistent modes. The P-Persistent mode defines that each node senses the channel, and if the channel is inactive, it sends a frame with a **P** probability. If the data is not transmitted, it waits for a (**q = 1-p probability**) random time and resumes the frame with the next time slot.

O- Persistent: It is an O-persistent method that defines the superiority of the station before the transmission of the frame on the shared channel. If it is found that the channel is inactive, each station waits for its turn to retransmit the data.



CSMA/ CD

It is a **carrier sense multiple access/ collision detection** network protocol to transmit data frames. The CSMA/CD protocol works with a medium access control layer. Therefore, it first senses the shared channel before broadcasting the frames, and if the channel is idle, it transmits a frame to check whether the transmission was successful. If the frame is successfully received, the station sends another frame. If any collision is detected in the CSMA/CD, the station sends a jam/ stop signal to the shared channel to terminate data transmission. After that, it waits for a random time before sending a frame to a channel.

CSMA/ CA

It is a **carrier sense multiple access/collision avoidance** network protocol for carrier transmission of data frames. It is a protocol that works with a medium access control layer. When a data frame is sent to a channel, it receives an acknowledgment to check whether the channel is clear. If the station receives only a single (own) acknowledgments, that means the data frame has been successfully transmitted to the receiver. But if it gets two signals (its own and one more in which the collision of frames), a collision of the frame occurs in the shared channel. Detects the collision of the frame when a sender receives an acknowledgment signal.

Following are the methods used in the CSMA/ CA to avoid the collision:

Interframe space: In this method, the station waits for the channel to become idle, and if it gets the channel is idle, it does not immediately send the data. Instead of this, it waits for some time, and this time period is called the **Interframe** space or IFS. However, the IFS time is often used to define the priority of the station.

Contention window: In the Contention window, the total time is divided into different slots. When the station/ sender is ready to transmit the data frame, it chooses a random slot number of slots as **wait time**. If the channel is still busy, it does not restart the entire process, except that it restarts the timer only to send data packets when the channel is inactive.

Acknowledgment: In the acknowledgment method, the sender station sends the data frame to the shared channel if the acknowledgment is not received ahead of time.

B. Controlled Access Protocol

It is a method of reducing data frame collision on a shared channel. In the controlled access method, each station interacts and decides to send a data frame by a particular station approved by all other stations. It means that a single station cannot send the data frames unless all other stations are not approved. It has three types of controlled access: **Reservation, Polling**, and **Token Passing**.

Reservation

Whenever we travel from a train or an airplane, the first thing we do is to reserve our seats, similarly here a station must make a reservation first before transmitting any data-frames. This reservation timeline consists of two kinds of periods:

1. Reservation interval of a fixed time duration
2. Data transmission period of variable frames

Consider there are 4 stations then the reservation intervals are divided into 4 slots so that each station has a slot. Means if n number of stations are there then n slot will be allotted.

Now let us assume that these 4 stations are 4 friends, now is friend-1 speaks in his slot-1 then no other friend can speak at this time. Similarly, if station-1 transmits a 1-bit data-frame in slot-1 then at that time no other station can transmit its data-frames and they must wait for their time slot. After all the slots have transmitted and checked then each station knows which station now wishes for transmission.

The biggest advantage of this method is since all stations agree on which station is next to transmit then there are no possible collisions.

The illustration below shows a scenario with five stations with a five-slot reservation frame. here, in the time interval station 1,3,4 are the only stations with reservations and in the second interval station-1 is the only station with a reservation.

Polling

In a computer network there is a primary station or controller (teacher) and all other stations are secondary (students), the primary station sends a message to each station. The message which is sent by the primary station consists of the address of the station which is selected for granting access.

The point to remember is that all the nodes receive the message but the addressed one responds and sends data in return, but if the station has no data to transmit then it sends a message called **Poll Reject or NAK** (negative acknowledgment).

But this method has some drawbacks like the high overhead of the polling messages and high dependence on the reliability of the primary station.

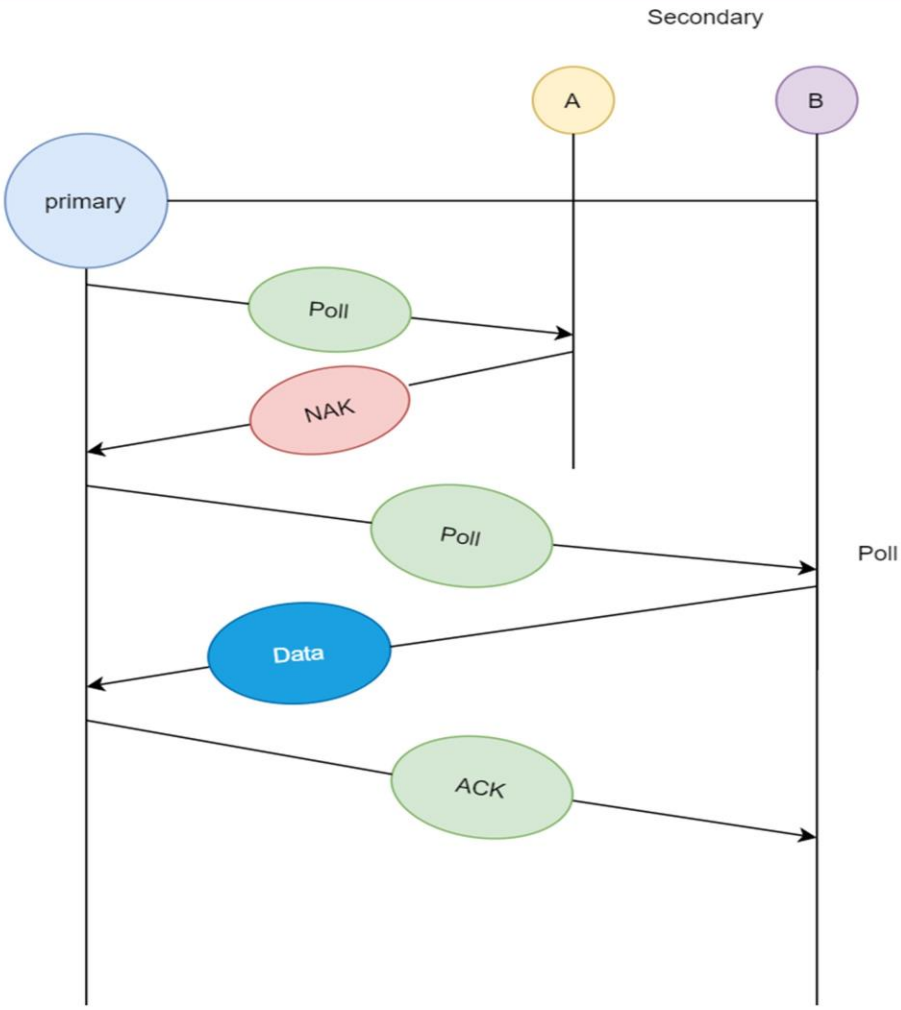
We calculate the efficiency of this method in terms of time for polling & time required for transmission of data.

Tpoll = time for polling

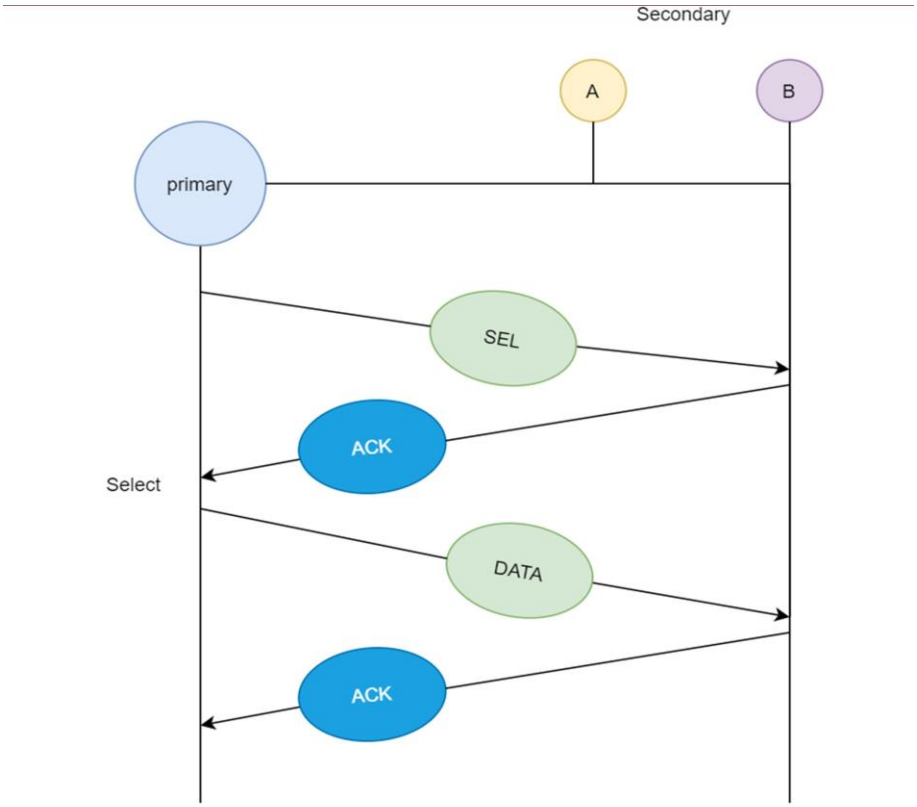
Tt = time required for transmission of data

So, **efficiency = Tt / (Tt + Tpoll)**

Whenever the primary station wants to recieve the data, it asks the secondary stations present in its channel, this method is **polling**. In the first diagram, we see that primary station asks station A if it has any data ready for transmission, since A does not have any data queued for transmission it sends NAK (negative acknowledgement), and then it asks station B, since B has data ready for transmission, so it transmits the data and in return recieves acknowledgement from primary station.



In the next case, if primary station wants to send data to the secondary stations, it sends a select message, and if the secondary station accepts the request from the primary station, then it sends back an acknowledgement and then primary station transmits the data and inreturn recieves an acknowledgement.



Token Passing

In computer networks a token is a special bit pattern that allows the token possessing system to send data or we can say that a token represents permission to transmit data. The token circulation around the table (or a network ring) is in a predefined order. A station can only pass the token to its adjacent station and not to any other station in the network. If a station has some data queued for transmission it can not transmit the data until it receives the token and makes sure it has transmitted all the data before passing on the received token.

This method has some drawbacks like duplication of token or sometimes the token is damaged or lost during the circulation, or some times if we introduce a new station or remove an existing station from the network, this leads to a huge disturbance, which should be taken care of so that the efficiency of the method is not affected.

The performance of a token ring is governed by 2 parameters, which are delay and throughput.

Delay is a measure of the time; it is the time difference between a packet ready for transmission and when it is transmitted. Hence, the average time required to send a token to the next station is a/N.

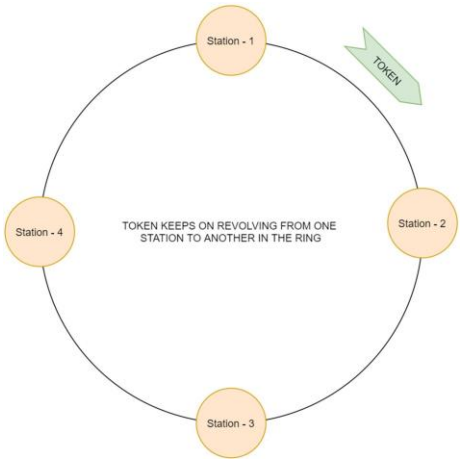
Throughput is a measure of the successful traffic in the communication channel.

Throughput, S = 1/ (1 + a/N) for a<1

S = 1/[a(1+1/N)] for a>1, here N = number of stations & a = Tp/Tt

Tp = propagation delay &Tt = transmission delay

In the diagram below when station-1 posses the token it starts transmitting all the data-frames which are in it's queue. now after transmission, station-1 passes the token to station-2 and so on. Station-1 can now transmit data again, only when all the stations in the network have transmitted their data and passed the token.



C. Channelization Protocols

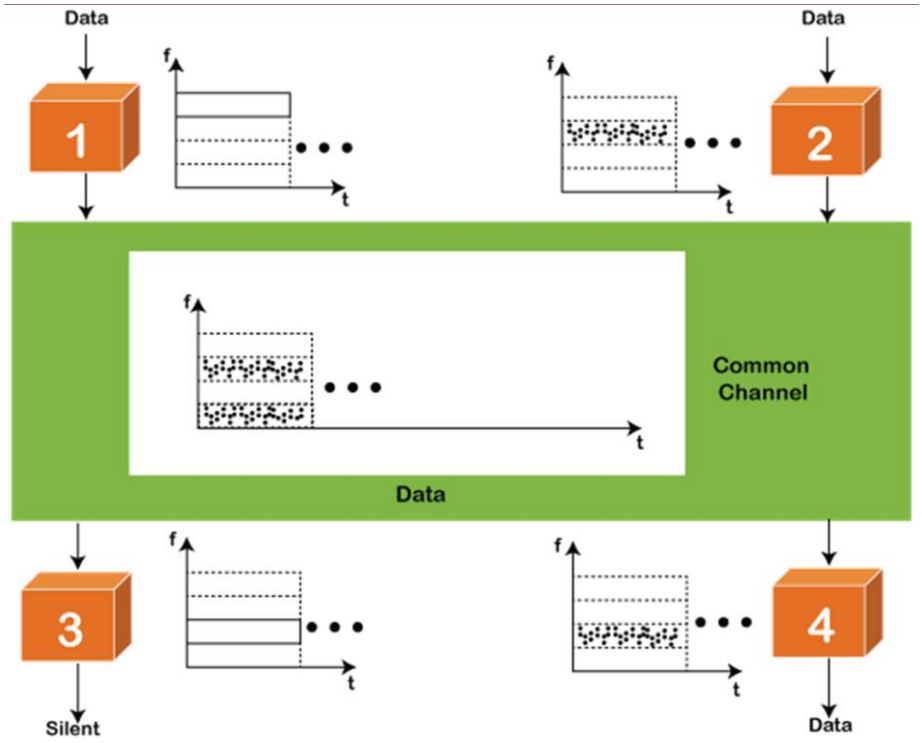
It is a channelization protocol that allows the total usable bandwidth in a shared channel to be shared across multiple stations based on their time, distance and codes. It can access all the stations at the same time to send the data frames to the channel.

Following are the various methods to access the channel based on their time, distance and codes:

1. **FDMA (Frequency Division Multiple Access)**
2. **TDMA (Time Division Multiple Access)**
3. **CDMA (Code Division Multiple Access**)

FDMA

It is a frequency division multiple access (**FDMA**) method used to divide the available bandwidth into equal bands so that multiple users can send data through a different frequency to the subchannel. Each station is reserved with a particular band to prevent the crosstalk between the channels and interferences of stations.



TDMA

Time Division Multiple Access (**TDMA**) is a channel access method. It allows the same frequency bandwidth to be shared across multiple stations. And to avoid collisions in the shared channel, it divides the channel into different frequency slots that allocate stations to transmit the data frames. The same **frequency** bandwidth into the shared channel by dividing the signal into various time slots to transmit it. However, TDMA has an overhead of synchronization that specifies each station's time slot by adding synchronization bits to each slot.

CDMA

The code division multiple access (CDMA) is a channel access method. In CDMA, all stations can simultaneously send the data over the same channel. It means that it allows each station to transmit the data frames with full frequency on the shared channel at all times. It does not require the division of bandwidth on a shared channel based on time slots. If multiple stations send data to a channel simultaneously, their data frames are separated by a unique code sequence. Each station has a different unique code for transmitting the data over a shared channel. For example, there are multiple users in a room that are continuously speaking. Data is received by the users if only two-person interact with each other using the same language. Similarly, in the network, if different stations communicate with each other simultaneously with different code language.

6. BLUETOOTH

- Bluetooth is, with the infrared, one of the major wireless technologies developed to achieve WPAN.
- Bluetooth is a wireless LAN technology used to connect devices of different functions such as telephones, computers (laptop or desktop), notebooks, cameras, printers and so on.
- Bluetooth is an example of personal area network. Bluetooth project was started by SIG (Special Interest Group) formed by four companies IBM, Intel, Nokia and Toshiba for interconnecting computing and communicating devices using short-range, lower-power, inexpensive wireless radios.
- The project was named Bluetooth after the name of Viking king – Harald Blaat and who unified Denmark and Norway in 10th century.
- Nowadays, Bluetooth technology is used for several computer and non computer application:

    1. It is used for providing communication between peripheral devices like wireless mouse or keyboard with the computer.
    2. It is used by modern healthcare devices to send signals to monitors.
    3. It is used by modern communicating devices like mobile phone, PDAs, palmtops etc to transfer data rapidly.
    4. It is used for dial up networking. Thus allowing a notebook computer to call via a mobile phone.
    5. It is used for cordless telephoning to connect a handset and its local base station.
    6. It also allows hands-free voice comml1nication with headset.
    7. It also enables a mobile computer to connect to a fixed LAN.
    8. It can also be used for file transfer operations from one mobile phone to another.
    9. Bluetooth uses omni directional radio waves that can through walls or other non-metal barriers.
    10. Bluetooth devices have a built-in short range radio transmitter. The rate provided is 1Mbps and uses 2.4 GHz bandwidth.

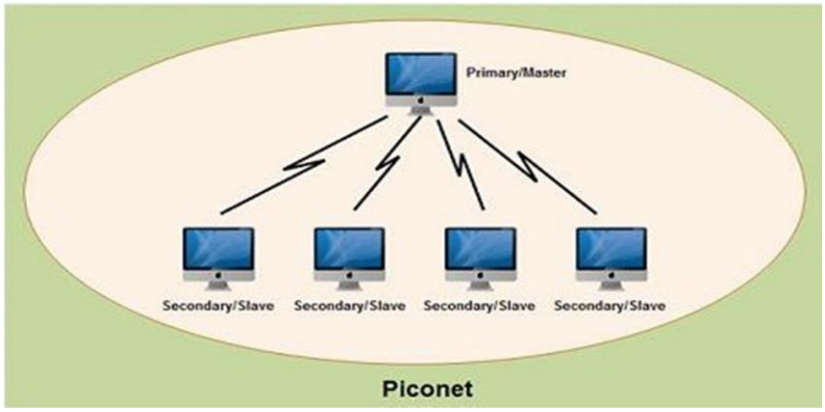
Bluetooth is that when the device is within the scope of a other devices automatically start the transfer information without the user noticing. A small network between the devices is created and the user can accessed as if there were cables.

Bluetooth architecture defines two types of networks:

1. Piconet
2. Scattemet

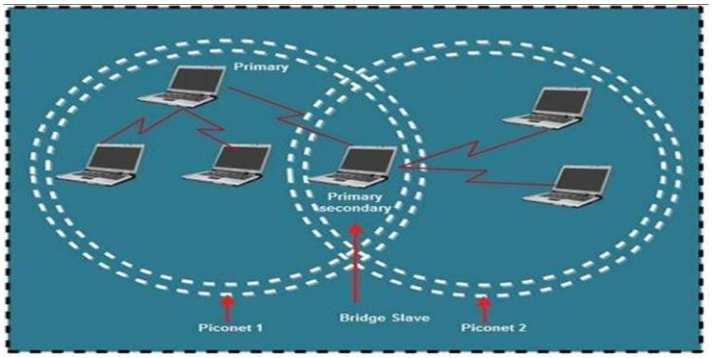
1. Piconet

- Piconet is a Bluetooth network that consists of one primary (master) node and seven active secondary (slave) nodes.
- Thus, piconet can have up to eight active nodes (1 master and 7 slaves) or stations within the distance of 10 meters.
- There can be only one primary or master station in each piconet.
- The communication between the primary and the secondary can be one-to-one or one-to-many.
- All communication is between master and a slave. Salve-slave communication is not possible.
- In addition to seven active slave station, a piconet can have up to 255 parked nodes. These parked nodes are secondary or slave stations and cannot take part in communication until it is moved from parked state to active state.



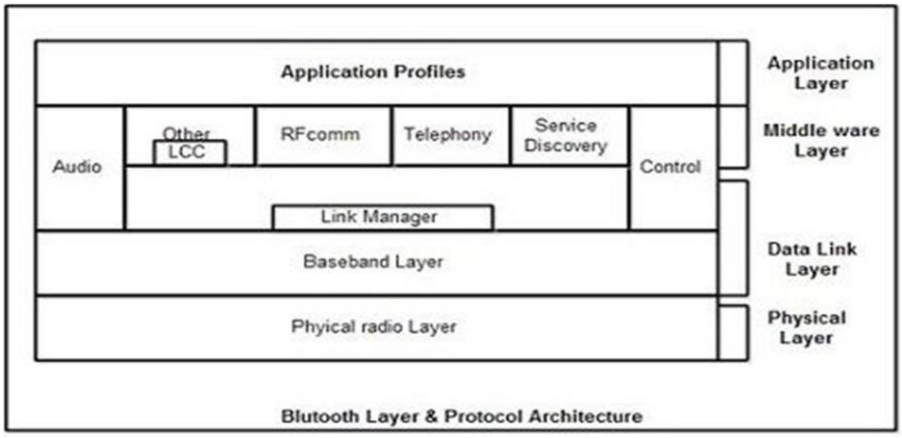
2. Scatternet

- Scattemet is formed by combining various piconets.
- A slave in one piconet can act as a master or primary in other piconet.
- Such a station or node can receive messages from the master in the first piconet and deliver the message to its slaves in other piconet where it is acting as master. This node is also called bridge slave.
- Thus a station can be a member of two piconets.



Bluetooth layers and Protocol Stack

- Bluetooth standard has many protocols that are organized into different layers.
- The layer structure of Bluetooth does not follow OS1 model, TCP/IP model or any other known model.
- The different layers and Bluetooth protocol architecture.



Radio Layer

- The Bluetooth radio layer corresponds to the physical layer of OSI model.
- It deals with ratio transmission and modulation.
- The radio layer moves data from master to slave or vice versa.
- It is a low power system that uses 2.4 GHz ISM band in a range of 10 meters.
- This band is divided into 79 channels of 1MHz each. Bluetooth uses the Frequency Hopping Spread Spectrum (FHSS) method in the physical layer to avoid interference from other devices or networks.
- Bluetooth hops 1600 times per second, i.e. each device changes its modulation frequency 1600 times per second.
- In order to change bits into a signal, it uses a version of FSK called GFSK i.e. FSK with Gaussian bandwidth filtering.

Baseband Layer

- Baseband layer is equivalent to the MAC sublayer in LANs.
- Bluetooth uses a form of TDMA called TDD-TDMA (time division duplex TDMA).
- Master and slave stations communicate with each other using time slots.
- The master in each piconet defines the time slot of 625 μsec.
- In TDD- TDMA, communication is half duplex in which receiver can send and receive data but not at the same time.
- If the piconet has only no slave; the master uses even numbered slots (0, 2, 4, …) and the slave uses odd-numbered slots (1, 3, 5, ….). Both master and slave communicate in half duplex mode. In slot 0, master sends & secondary receives; in slot 1, secondary sends and primary receives.
- If piconet has more than one slave, the master uses even numbered slots. The slave sends in the next odd-numbered slot if the packet in the previous slot was addressed to it.
- In Base-band layer, two types of links can be created between a master and slave. These are:

1. Asynchronous Connection-less (ACL)

- It is used for packet switched data that is available at irregular intervals.
- ACL delivers traffic on a best effort basis. Frames can be lost & may have to be re-transmitted.
- A slave can have only one ACL link to its master.
- Thus ACL link is used where correct delivery is preferred over fast delivery.
- The ACL can achieve a maximum data rate of 721 kbps by using one, three or more slots.

2. Synchronous Connection Oriented (SCO)

- sco is used for real time data such as sound. It is used where fast delivery is preferred over accurate delivery.
- In an sco link, a physical link is created between the master and slave by reserving specific slots at regular intervals.
- Damaged packet; are not re-transmitted over sco links.
- A slave can have three sco links with the master and can send data at 64 Kbps.

Logical Link, Control Adaptation Protocol Layer (L2CAP)

- The logical unit link control adaptation protocol is equivalent to logical link control sub-layer of LAN.
- The ACL link uses L2CAP for data exchange but sco channel does not use it.
- The various function of L2CAP is:

1. **Segmentation and reassembly**

- L2CAP receives the packets of up to 64 KB from upper layers and divides them into frames for transmission.
- It adds extra information to define the location of frame in the original packet.
- The L2CAP reassembles the frame into packets again at the destination.

2. **Multiplexing**

- L2CAP performs multiplexing at sender side and de-multiplexing at receiver side.

• At the sender site, it accepts data from one of the upper layer protocols frames them and deliver them to the Base-band layer.

• At the receiver site, it accepts a frame from the base-band layer, extracts the data, and delivers them to the appropriate protocol1ayer.

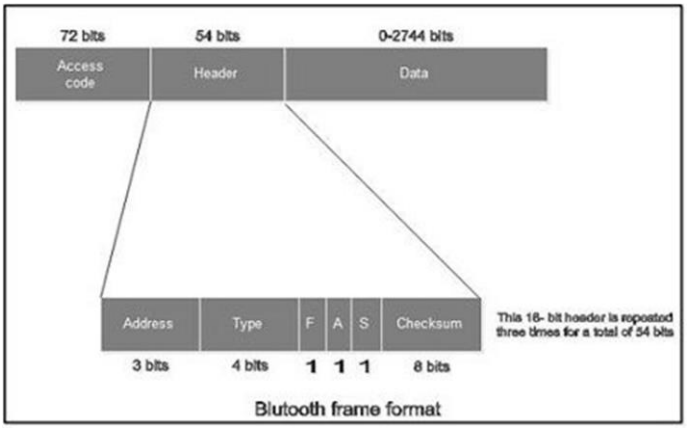
3. **Quality of Service (QOS)**

• L2CAP handles quality of service requirements, both when links are established and during normal operation.

• It also enables the devices to negotiate the maximum payload size during connection establishment.

Bluetooth Frame Format

The various fields of blue tooth frame format are:



Blutooth frame format

1. Access Code: It is 72 bit field that contains synchronization bits. It identifies the master.

2. Header: This is 54-bit field. It contain 18 bit pattern that is repeated for 3 time.

The header field contains following sub-fields:

(i) Address: This 3 bit field can define up to seven slaves (1 to 7). If the address is zero, it is used for broadcast communication from primary to all secondaries.

(ii) Type: This 4 bit field identifies the type of data coming from upper layers.

(iii) F: This flow bit is used for flow control. When set to 1, it means the device is unable to receive more frames.

(iv) A: This bit is used for acknowledgement.

(v) S: This bit contains a sequence number of the frame to detect re-transmission. As stop and wait protocol is used, one bit is sufficient.

(vi) Checksum: This 8 bit field contains checksum to detect errors in header.

3. Data: This field can be 0 to 2744 bits long. It contains data or control information coming from upper layers